**Document Code No.:** ITG-P-07-01-01
**Title: Extended Network and Systems Connectivity Policy**
**Affected Agencies:**
**Authorities:** KCC 2A.380.070
**Keywords:** SSL, SSA, Network, Remote Access, LAN, WAN, Public Key, Cryptography, Symmetric-Key, VPN, User ID, Username, IPsec, IGN, Internet, Firewall, EAP, Access Control, Anti-Virus
**Sponsoring Agency:** Department of Information Technology

King County

**Chief Information Officer signature:** DocuSigned by: _____
**Date signed and effective:** 10/17/2018 920AF9FCB611460... _____

---

## I. Purpose:

This policy is designed to minimize the potential exposure to King County from damages that may result from authorized or unauthorized use of King County resources. Theses damages include the exposure or loss of sensitive and confidential information, intellectual property harm to public image, and damage to critical King County internal systems, etc.

This policy provides the approved methods for accessing the King County Enterprise Network from external networks or hosts.

## II. Applicability and Audience

This policy applies to all King County Organizations, Workforce Members, and non-County Users (NCU) who are connectivity to the King County Enterprise Network and using King County Information Assets.

[*Note:* IT Governance Policies apply to the Executive Branch. Applicable to independently elected agencies as baseline policy requirements.]

## III. Definitions

a. **Access Control Mechanism:** Access control systems perform authorization identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and electronic keys.
b. **Agreement:** Any document detailing the specifics of a relationship between parties. Examples include, but are not limited to, contracts, memorandums of understanding (MOU), memorandums of agreement (MOA), King County Access Agreement, or service level agreements (SLA).
c. **Anti-Virus Software:** Computer software used to prevent, detect and remove malicious software, including but not limited to viruses, ransomware, key loggers, Trojan horses, worms, adware, spyware, etc.
d. **Authentication Framework:** Extensible Authentication Protocol (EAP) which is a framework included in Windows Client and Windows Server operating systems. EAP in Windows includes many authentication protocols for network access authentication when you deploy dial-up, virtual private network (VPN), 802.1X wireless, and 802.1X wired technologies using Network Policy Server
e. **Business Partner:** Outside businesses associated or "partnered" with a Vendor doing business with King County.
f. **Due Care:** The care that a reasonable person would exercise under the circumstances; the standard for determining legal duty.

g. **Firewall:** A part of a computer system or network that is designed to block unauthorized access while permitting authorized communication. A firewall is designated as a buffer between any connected public Network and a private Network.
h. **Idle:** Describes a computing circumstance in which there is no keyboard activity, no applications are running and nothing is being uploaded or downloaded.
i. **Information Asset:** A definable piece of information, information processing equipment,
j. or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:
    a. Not easily replaced without cost, skill, time, resources, or a combination,
    b. Part of the Organization's identity, without which, the Organization may be threatened.
k. **Information Owner:** The person who is responsible for protecting an Information Asset, maintaining the accuracy and integrity of the Information Asset, determining the appropriate data sensitivity or classification level for the Information Asset and regularly reviewing its level for appropriateness, and ensuring the Information Asset adheres to policy. The Information Owner is one or both of the following:
    a. The creator of the information or the manager of the creator of the information
    b. The receiver of external information or the manager of the receiver of the external information
l. **Internet:** (Upper case "I" - Internet) The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.
m. **Internet Protocol Security (IPsec):** A protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).[1] Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality (encryption), and replay protection.
n. **Intergovernmental Network (KC IGN):** The statewide closed network inter-connecting municipalities, counties, and the state to enable the sharing of information among employees and work groups.
o. **King County Enterprise Network:** The Network used to conduct county business that provides transport of data within and between county facilities and other agencies of county government. This definition also refers to the Network used to transport data between the county, other government agencies and the Internet. It does not refer to Networks built for the sole purpose of meeting special operations needs of county business units, including process control and supervisory control networks (SCADA), Nor does it refer to the King County Institutional Network (I-Net), which is required to meet contractual obligations with I-Net customers and the local cable television utility.

p. **King County Wide Area Network (KC WAN):** See King County Enterprise Network
q. **Least Privilege:** Granting a user only those access rights needed to perform official job duties.
r. **Local Area Network (LAN):** A computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building and has its network equipment and interconnects locally managed.
s. **Login or Logon:** The process of gaining access, or signing in to a computer system. The process (the noun) is a "logon" or "login," while the act of doing it (the verb) is to "log on" or "log in."
t. **Network:** A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet
u. **Organization:** Every county office, every officer, every institution' whether educational, correctional or other; and every department, division, board, and commission.
v. **Password:** A confidential sequence of characters used to authenticate an individual's identity, usually during a logon process.
w. **Public Key Cryptography:** Any of various techniques that use two different keys whereby data encrypted with one key can only be decrypted using the other. In typical use, the recipient makes one key public and keeps the other private, so that anyone may encrypt data for the recipient, but only the recipient can decrypt it.
x. **Public Record:** A Public Record includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used or retained by an agency regardless of physical form or characteristics.
y. **Remote Access:** The ability to log on to a secure computer or Network within an organization from an external non-county location. Remote Access is accomplished via a connection to the Internet using either a web-browser (SSL) interface or installed client software to maintain security of data in transit.
z. **Remote Access Profile:** An King County Information and Technology (KCIT) form that describes the type of access allowed and what King County resources are available to the Workforce Member.
aa. **Resources:** Assets that can be used for help or support that can be drawn on when needed.
bb. **Secure Sockets Layer (SSL):** The leading security protocol on the Internet. SSL is widely used to do two things: to validate the identity of a Web site and to create an encrypted connection between devices. SSL is cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over
cc. **Service Level Agreement (SLA):** A formal agreement that outlines the roles, responsibilities, procedures, and expectations shared between two parties.
dd. **Symmetric-Key Cryptosystem:** Algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link

ee. **System:** software, hardware, and interface components that work together to perform a set of business functions.

ff. **Users:** Any individual performing work for King County utilizing a personal computer, workstation or terminal, including but not limited to: any employee, contractor, consultant, vendor, Business Partner or other worker.

gg. **User ID or Username:** A unique code or string of characters used to identify a specific user. Also known as user accounts.

hh. **Vendor:** A person or entity who is a seller of products or services to a King County Organization. Vendors can also be Workforce Members.

ii. **Virtual Private Network (VPN):** A virtual private network extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

jj. **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates- associates' students, volunteers, and staff from third party entities who provide services to King County.

## IV. Policy

A. General

1. Approved Access Methodologies

a. All Workforce Members are required to use only Remote Access methodologies approved by King County Information Technology (KCIT) department and the Chief Information Security and Privacy Officer (CISPO).

b. Virtual Private Networks (VPN) shall follow the IP Security (IPsec) or Secure Socket Layer (SSL) standard and uses a public-key 2048 bit or symmetrical- key 256 bit cryptographic key strength.

c. Access to the county's Networks is based on the concept of Least Privilege. Some form of Access Control Mechanism shall control all access to private, sensitive, proprietary, copyrighted or licensed information.

d. Network protocols used to transport traffic on the King County Enterprise Network shall be restricted according to rules described in the Network Administration Standard.

e. The authentication framework shall be appropriate for the classification of the data being processed.

f. The county shall not be liable for the accuracy of data transmitted over the Internet.

g. Non-County Users (NCUs), with an identifiable, justifiable, and ongoing business need may be provided access to King County's internal resources and services by way of a Network connection to the KC WAN or KC IGN. This access shall be based on formal King County Access Agreement between the NCU and county,

through KCIT and department or agency providing the applications as outlined in the external network connections standard.

h. Approved Remote Access Workforce Members shall not permit unauthorized access by others, including family members, to the county computing environment.

i. Remote Access Workforce Members shall not share their Remote Access credentials with anyone.

2. Security

   a. NCUs shall conform to the county's Network and security standards while connected to county Networks, in an accordance with the King County Information Security Policy

   b. The NCU shall be responsible for its own security requirements.

   c. Loss, compromise, or suspected loss or compromise, of the Access Control Mechanism shall be immediately reported to the King County Information Technology (KCIT) Customer Support Services.

   d. Employees with Remote Access privileges shall take due care to protect the assets of King County. Remote Access Employees are accountable to adhere to the county's information security policy, standards and guidelines. Being approved for Remote Access does not diminish the responsibility of adhering to all provisions of security policies; in fact the responsibility is greater when working remotely. If the Workforce Member is uncertain of their level of risk through using Remote Access he or she should contact Information Security, Risk & Compliance (ISRC)

3. Remote Access

   a. No Workforce Members shall be granted Remote Access to the King County Enterprise Network resources except in accordance with a demonstrated need and permission from the proper authorities.

      i. The proper authorities for Workforce Members are the King County Information Owners.

   b. Remote Access Workforce Members may be provided access to the same Systems and resources they currently access non-remotely. However, Workforce Members may receive a lesser degree of access via Remote Access methods, dependent upon the clearance received when their Remote Access is granted. In no case shall Remote Access Workforce Members be granted a greater degree of access than they are allowed via their direct connection.

   c. Selected consultants and vendors may be granted Remote Access to the King County Enterprise Network, provided they have an approved and signed King County Access Agreement that clearly defines the type and scope of access permitted, and they meet requirements, such as Anti-Virus protection software.

   d. King County shall reserve the right to electronically examine all devices connecting to the King County Enterprise Network prior to granting access to the Network.

e. The Remote Access (Network Level access) workforce Member is responsible for ensuring his or her personal computer has Anti-Virus Software running and is current with the engine and data files for the Vendor software used' The Anti-Virus Software should be updated weekly, at a minimum, and preferably once a day.

f. For the Workforce Member's protection and that of the System, Workforce Members shall follow the King County Password Management Policy.

i. If your Remote Login information is stolen, compromised or potentially compromised, inform KCIT Customer Support Services immediately.

g. All locally installed host applications and/or services required for Remote Access shall be set up for manual start and stop. Services shall be left in a stopped status when not in use.

h. While using Remote Access Network Level Access, Workforce Members are required to disconnect from the King County Enterprise Network whenever their computer Systems are Idle for greater than thirty (30) minutes.

i. Continuously active Remote Access connections exceeding 9 hours will be disconnected and require user to reconnect for access.

j. King County is not responsible for the purchase, set-up, maintenance or support of any equipment that is not owned by or leased to King County.

4. Remote Access for King county employees may be allowed through the use of equipment owned by or leased to King County, or through the use of the employee's personal computer System, unless otherwise restricted by the Organization or Information Owner.

a. "If a personal computer is used for any County business, it could be subject to electronic discovery rules during a lawsuit o¡ the Washington Public Records Act. Any work-related emails, files, data or other record residing on a personal computer is subject to the same retention requirements as records on a County computer"' (From PAO Memorandum of 1 August 2007.)

5. External NCU's requests for a Network connection to county services shall meet the following approval criteria before being granted:

a. The director of the Organization that owns the county service or system has determined that sufficient direct business benefit for the county and NCU exists to justify providing a secure Network connection. The director will provide a business justification prior to any connectivity.

b. The NCU shall agree in writing to abide both in fact and spirit, to the King County Network access and security policies.

B. Administration

1. A request to make changes to a workforce Member's Remote Access profile shall originate with his or her manager or supervisor.

2. Immediate supervisors and division managers shall setup Remote Access agreements so they expire on a routine basis, up to a maximum of twelve (12)

months. At the expiration of a Remote Access Agreement the employee would have the option of requesting a renewal.

3. When a Workforce Member leaves the employ of King County Remote Access shall be disabled immediately.
4. KCIT, the requesting Organization, and the NCU shall complete a King County Access Agreement outlining the responsibilities, expectations, access details, and contacts.
5. The King County Access Agreements shall be reviewed by KCIT and the requesting Organization, on an annual basis to ensure existing configurations and arrangements remain valid and justifiable.

## V. Implementation Plan

A. This policy becomes effective for Executive Branch agencies on the date that it is signed by the County Chief Information Officer. KCIT Production Operations is responsible for implementation of this policy.

B. King County Departments and Agencies are responsible for communicating this policy to the management structure within their respective agencies and other appropriate parties.

## VI. Maintenance

A. This policy will be maintained by KCIT Production Operations

B. This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by KCIT Production Operations prior to the expiration date.

## VII. Consequences for Noncompliance

A. Failure to comply will result is the denial and/or revocation of Remote Access or External Connectivity until compliance can be obtained.

## VIII. Appendices: [*Note*: List Appendices using formal titles.]